SONICWALL

Email Security - urządzenia i oprogramowanie

Chroń swoją infrastrukturę przed zaawansowanymi atakami na pocztę e-mail oraz zapobiegaj naruszeniom zgodności z przepisami przy użyciu skutecznych i łatwych w użyciu rozwiązań

Poczta e-mail jest podstawą komunikacji biznesowej i dlatego stanowi główny cel cyberataków, w tym wykorzystujących złośliwe oprogramowanie ransomware, phishing, techniki BEC (Business Email Compromise), spoofing, spam i wirusy. Co więcej, przepisy prawne zmuszają organizacje do ochrony poufnych danych i dbania o to, by nie dochodziło do ich wycieku, a poczta zawierająca wrażliwe informacji na temat klientów była przekazywana w sposób bezpieczny. Bez względu na to, czy chodzi o rozwijającą się firmę z sektora małych i średnich przedsiębiorstw, dużą i rozproszoną korporację, czy dostawcę usług zarządzanych (MSP), każda organizacja wymaga ekonomicznego rozwiązania do ochrony i szyfrowania poczty e-mail. Takiego, które będzie się łatwo skalować, umożliwiając zwiększenie pojemności systemu oraz delegowanie zarządzania między jednostkami organizacyjnymi i domenami.

Specjalizowane urządzenia oraz oprogramowanie SonicWall Email Security zapewniają wielowarstwową ochronę poczty e-mail przed zewnętrznymi i wewnętrznymi atakami oraz naruszeniami zgodności z przepisami. Rozwiązanie skanuje całą zawartość przychodzących i wychodzących wiadomości, adresy URL i załączniki pod kątem poufnych danych, chroniąc w czasie rzeczywistym przed takimi zagrożeniami, jak: ransomware, ukierunkowane ataki phishingowe, spoofing, wirusy, złośliwe adresy URL, zombie, DHA (Directory Harvest Attack), DoS (Denial of Service) i inne. SonicWall Email Security wykorzystuje wiele opatentowanych firmowych technik wykrywania zagrożeń oraz unikatową, globalną sieć identyfikującą i monitorującą ataki.

Usługa SonicWall Capture Advanced Threat Protection oferuje wiodący w branży, wielosilnikowy sandboxing, wsparty zgłoszoną do opatentowania technologią RTDMI™ (Real-Time Deep Memory Inspection), zapewniając izolowanie nieznanych dotąd zagrożeń identyfikowanych w podejrzanych plikach załączników oraz adresach URL. Dzięki temu blokuje zaawansowane zagrożenia, zanim dotrą do skrzynek odbiorczych użytkowników. Oparta na Capture ATP ochrona poczty e-mail szybko i skutecznie zabezpiecza przed ransomware i atakami typu zero-day.

Rozwiązanie obejmuje także techniki Domain-based Message Authentication, DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) oraz Reporting and Conformance (DMARC), zapewniając niezwykle skuteczną metodę uwierzytelniania wiadomości e-mail. W rezultacie potrafi wykrywać sfałszowaną pocztę, ograniczać spam i chronić przed takimi ukierunkowanymi atakami phishingowymi, jak spear-phishing, whaling, CEO fraud oraz BEC (Business Email Compromise). Powiadamia także o źródłach i nadawcach wiadomości e-mail, dzięki czemu możemy identyfikować i blokować nieautoryzowanych i fałszujących nasz firmowy adres e-mail nadawców, chroniąc swoją markę. Ponadto zapobiega wyciekowi poufnych danych i naruszeniom przepisów prawa, dzięki zaawansowanemu skanowaniu i zarządzaniu zgodnością, a także zintegrowanej, opartej na chmurze usłudze szyfrującej pocztę e-mail, zapewniającej bezpieczną wymianę poufnych danych.

Administrowanie rozwiązaniem Email Security jest intuicyjne, szybkie i proste. Można bezpiecznie przekazać zarządzanie spamem użytkownikom końcowym, zachowując jednocześnie pełną kontrolę nad egzekwowaniem ochrony. Można także łatwo zarządzać kontami użytkowników i grup dzięki płynnej synchronizacji wielu katalogów LDAP. Dzięki obsłudze architektury multi-tenant w dużych, rozproszonych środowiskach możliwe jest w ramach jednego wdrożenia rozwiązania Email Security delegowanie administratorów niższego poziomu do zarządzania ustawieniami w różnych jednostkach organizacyjnych (takich jak oddziały przedsiębiorstw lub klienci dostawców MSP) .

Korzyści

- Oparta na Capture ATP ochrona skrzynek pocztowych przed zaawansowanymi zagrożeniami, takimi jak ransomware i złośliwe oprogramowanie typu zero-day
- Zapobieganie klikaniu złośliwych linków przez użytkowników na dowolnych urządzeniach i w dowolnej lokalizacji
- Zaawansowane techniki analizy zapobiegające ukierunkowanemu phishingowi, oszustwom wykorzystującym wiadomości e-mail oraz atakom BEC (Business Email Compromise)
- Powstrzymywanie nowych zagrożeń dzięki aktualizowanym w czasie rzeczywistym wynikom analiz SonicWall Capture Labs
- Utrzymywanie higieny poczty e-mail przy użyciu efektywnej ochrony antyspamowej i antywirusowej
- Ochrona informacji dzięki szczegółowym politykom zapobiegania utracie danych (DLP) i utrzymania zgodności z przepisami
- Uproszczone zarządzanie dzięki inteligentnej automatyzacji, delegowaniu zadań, przejrzystej i dostosowywanej konsoli oraz obszernemu raportowaniu
- Elastyczne i skalowalne opcje wdrażania, obejmujące dodatkowo zabezpieczone urządzenia fizyczne, wydajne urządzenia wirtualne oraz funkcjonalny system Windows Server
-

[1] *U.S. Patents 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348*

Funkcje

Capture Advance Threat Protection

Wykrywaj i blokuj potencjalne zaawansowane zagrożenia do momentu otrzymania wyniku ich analizy. Usługa Capture ATP to jedyna metoda wykrywania zaawansowanych zagrożeń, która łączy wielowarstwowy sandboxing z techniką Real-Time Deep Memory Inspection, pełną emulacją systemu oraz wirtualizacją w celu analizy zachowania podejrzanego kodu w wiadomościach e-mail. W rezultacie chroni użytkowników przed rosnącym zagrożeniem związanym z atakami typu zero-day. Usługa obejmuje zaawansowaną ochronę URL, która dynamicznie analizuje osadzone w wiadomościach adresy internetowe, blokując i poddając kwarantannie pocztę ze złośliwymi odnośnikami, zanim dotrą one do skrzynki odbiorczej. W rezultacie użytkownicy nie mogą na nich kliknąć i są chronieni przed naruszeniami bezpieczeństwa. Capture ATP zapewnia większą skuteczność ochrony, dzięki analizie załączników i adresów URL, możliwościom szczegółowego raportowania i uproszczonej obsłudze użytkownika.

Dodatkowo, SonicWall Email Security przepisuje wszystkie osadzone linki w celu blokowania wiadomości e-mail zawierających złośliwe lub phishingowe adresy URL. W efekcie użytkownicy są chronieni w momencie kliknięcia na dowolnym urządzeniu i w dowolnej lokalizacji.

Z powodu regulacji oraz potencjalnych opóźnień w komunikacji niektóre organizacje i instytucje rządowe mogą nie chcieć wykorzystywać opartych na chmurze technik inspekcji plików, takich jak Capture ATP. W tym wypadku rozwiązaniem staje się integracja urządzenia Email Security z rozwiązaniem SonicWall Capture Security appliance (CSa), umożliwiająca badanie podejrzanych plików przychodzących pocztą e-mail we własnym centrum danych. CSa może być powiązane z adresem IP lub FQDN, co czyni je doskonałym narzędziem do zapobiegania zagrożeniom.

Ochrona przed ukierunkowanymi atakami

Ochrona antyphishingowa SonicWall wykorzystuje połączenie różnych technologii, w tym uczenia maszynowego, heurystyki, oceny reputacji oraz analizy treści, powstrzymując wyrafinowane ataki. Rozwiązanie obejmuje również zaawansowane standardy uwierzytelniania wiadomości e-mail, takie jak SPF, DKIM i DMARC, w celu powstrzymywania ataków opartych na spoofingu, technikach BEC (Business Email Compromise) oraz zapobieganiu innym oszustwom wykorzystujących pocztę elektroniczną.

Analiza zagrożeń w czasie rzeczywistym

Korzystaj z najefektywniejszej i najbardziej aktualnej ochrony przed nowymi atakami spamowymi, opartej na informacjach uzyskiwanych z milionów źródeł danych w sieci SonicWall Capture Threat Network, zapewniając dostarczanie legalnych wiadomości e-mail. SonicWall Capture Labs analizuje informacje i przeprowadza rygorystyczne testy w celu oceny reputacji nadawców i treści, identyfikując nowe zagrożenia w czasie rzeczywistym.

Ochrona antywirusowa i antyspyware

Zyskaj stale aktualizowaną ochronę antywirusową i antyspyware. Wykorzystując sygnatury z wiodących w branży antywirusowych baz danych oraz wykrywanie złośliwych adresów URL, rozwiązanie zapewnia wielowarstwową ochronę, która jest skuteczniejsza od rozwiązań opartych na pojedynczej technologii antywirusowej.

Co więcej, dzięki analizie predykcyjnej sieć jest chroniona od chwili pojawienia się nowej odmiany wirusów do momentu udostępnienia aktualizacji sygnatur antywirusowych.

Inteligentna automatyzacja, delegowanie zadań i szczegółowe raportowanie

Uprość zarządzanie dzięki inteligentnej automatyzacji, delegowaniu zadań i szczegółowemu raportowaniu. Automatycznie zarządzaj adresami e-mail, kontami i grupami użytkowników. Bezproblemowo integruj ochronę poczty z wieloma serwerami LDAP. Wykorzystaj wtyczkę programową Junk Button for Outlook® do bezproblemowego przekazania zarządzania spamem użytkownikom końcowym, zachowując przy tym pełną kontrolę. Znajdź dowolny e-mail w ciągu kilku sekund dzięki wyszukiwarce Rapid Message Search Engine. Scentralizowane raportowanie (także w trybie split) dostarcza łatwe w dostosowywaniu, obejmujące cały system, a przy tym szczegółowe informacje o typach ataków, skuteczności ochrony i monitorowanej wydajności. Raporty są dostępne w formacie PDF i JPEG.

Zarządzanie politykami zgodności

Ta dodatkowa usługa zapewnia zgodność z przepisami i regulacjami, pomagając w identyfikowaniu, monitorowaniu oraz raportowaniu wiadomości e-mail naruszających standardy prawne i branżowe (np. HIPAA, SOX, GLBA i PCI-DSS) lub wytyczne dotyczące zapobieganiu utracie danych w firmie. Oferowana na zasadzie subskrypcji usługa umożliwia także routing poczty w oparciu o polityki zatwierdzenia, archiwizowania i szyfrowania wiadomości.

Szyfrowanie wiadomości e-mail

Wykorzystaj wydajny schemat zapobiegania wyciekom danych, a także zarządzania i egzekwowania wymagań zgodności oraz zapewniania bezpiecznej wymiany poczty na urządzeniach mobilnych w organizacji dowolnej wielkości.

W celu potwierdzenia godziny odbioru i otwarcia zaszyfrowana wiadomość e-mail może być śledzona. Obsługa szyfrowania jest intuicyjna: do skrzynki odbiorcy jest dostarczany e-mail z powiadomieniem i instrukcją, jak zalogować się do bezpiecznego portalu, aby przeczytać lub pobrać wiadomość. Usługa jest oparta na chmurze i - w odróżnieniu od konkurencyjnych rozwiązań - nie wymaga dodatkowego oprogramowania klienckiego. Do zaszyfrowanej wiadomości e-mail można uzyskać dostęp i odczytać ją z urządzeń mobilnych i laptopów.

Elastyczne wdrażanie

Uzyskaj długoterminowe, wynikające ze skalowania korzyści, konfigurując rozwiązanie z myślą o jego rozwoju i redundancji, przy minimalnych nakładach początkowych. Rozwiązanie Email Security można wdrożyć jako dodatkowo zabezpieczone, wydajne urządzenie fizyczne, jako oprogramowanie wykorzystujące istniejącą infrastrukturę albo jako urządzenie wirtualne na współdzielonych zasobach - co prowadzi do optymalizacji ich zużycia, ułatwia migrację i ogranicza wydatki inwestycyjne. Zacznij od jednego systemu, a następnie - w miarę rozwoju firmy - zwiększaj jego pojemność i rozwijaj odporną na awarię architekturę działającą w trybie split. Obsługa środowiska multi-tenant umożliwia dużym przedsiębiorstwom lub dostawcom usług zarządzanych (MSP) wdrożenia w wielu oddziałach lub dla wielu klientów oraz tworzenie jednostek organizacyjnych z jedną lub wieloma domenami. Wdrożenie może być zarządzane centralnie, ale jednocześnie każda jednostka organizacyjna może posiadać własnych użytkowników, administratorów niższego poziomu, reguły polityki, skrzynki na spam itp.

Opcje wdrażania SonicWall Email Security

Wyjątkowo elastyczna architektura sprawia, że SonicWall Email Security świetnie nadaje się do wdrażania w organizacjach wymagających wysoce skalowalnego, redundantnego i rozproszonego rozwiązania do ochrony poczty e-mail, którym można zarządzać centralnie. SonicWall Email Security można wdrożyć w trybie all-in-one lub split.

W trybie split systemy mogą być skonfigurowane jako zdalny analizator lub centrum sterowania. W typowym wdrożeniu w trybie split do centrum sterowania jest podłączonych jeden lub kilka zdalnych analizatorów. Zdalny analizator odbiera wiadomości e-mail z co najmniej jednej domeny i - wykorzystując zarządzanie połączeniami, filtrowanie wiadomości e-mail (antyspam, antyphishing i antywirus) oraz zaawansowane polityki - dostarcza legalne wiadomości do docelowego serwera pocztowego.

Centrum sterowania zarządza wszystkimi zdalnymi analizatorami oraz zbiera i przechowuje wiadomości-śmieci z tych analizatorów. Scentralizowane zarządzanie obejmuje raportowanie i monitorowanie wszystkich powiązanych systemów. Ten schemat działania ułatwia efektywne kosztowo skalowanie oraz ochronę zarówno przychodzącej, jak i wychodzącej poczty w rozwijających się organizacjach. Przy użyciu wirtualnych urządzeń SonicWall Email Security można w pełni wdrożyć tryb split na jednym lub wielu serwerach, uzyskując optymalną wydajność i skalowalność.

Funkcje	APPLIANCE, VIRTUAL APPLIANCE	WINDOWS SERVER®
Subskrypcja Advanced Total Secure - Advanced protection bundle		
Oprócz subskrypcji Total Secure obejmuje także SonicWall Capture ATP - zaawansowaną ochronę przed złośliwymi załącznikami i adresami URL	Tak	Tak
Ochrona przed klikaniem na złośliwych linkach	Tak	Tak
Subskrypcja Total Secure – Basic protection bundle		
Obejmuje subskrypcję dynamicznej ochrony e-mail 24/7 oraz funkcje wielowarstwowego antywirusa, detekcji złośliwych URL i zarządzania zgodnością z przepisami	Tak	Tak
Ochrona Ransomware & Zero-day - opcja		
SonicWall Capture ATP - zaawansowana ochrona przed złośliwymi załącznikami i adresami URL - jako dodatek do subskrypcji Total Secure	Tak	Tak
Kompletna ochrona poczty przychodzącej i wychodzącej		
Skuteczny antyspam	Tak	Tak
Zarządzanie połączeniami i zaawansowana ochrona reputacyjna IP	Tak	Tak
Detekcja, klasyfikacja i blokowanie phishingu	Tak	Tak
Ochrona przed atakami directory harvest, denial of service i NDR	Tak	Tak
Antyspoofing z obsługą SPF, DKIM i DMARC	Tak	Tak
Polityki dla użytkownika, grup, wszystkich	Tak	Tak
Agent in memory message transfer (MTA) w celu zwiększenia przepustowości	Tak	Tak
Łatwe administrowanie		
Instalacja	<1 godz.	<1 godz.
Zarządzanie w tygodniu	<10 min.	<10 min.
Automatyczny multi-LDAP sync dla użytkowników, grup	Tak	Tak
Kompatybilność ze wszystkimi serwerami SMTP	Tak	Tak
Obsługa SMTP Authentication (SMPT AUTH)	Tak	Tak
Kontrola allow/deny użytkownika końcowego	Tak	Tak
Dostosowywanie, harmonogramowanie i wysyłanie raportów 30+	Tak	Tak
Szczegóły werdyktu	Tak	Tak
Dostosowywana konsola zarządzania z całościowym wglądem	Tak	Tak
Szybki mechanizm wyszukiwania wiadomości	Tak	Tak
Skalowalna architektura w trybie split	Tak	Tak
Klastrowanie i zdalne klastrowanie	Tak	Tak
Łatwa obsługa dla użytkowników końcowych		
Single sign-on	Tak	Tak
Skrzynka na spam dla każdego użytkownika, wiadomości podsumowujące działania ze spamem	Tak	Tak
Agresywność antyspamu na użytkownika, listy block/allow	Tak	Tak
Subskrypcja ochrony email z wymaganym dynamicznym wsparciem		
Chmurowy antywirus, antyspam i antyphishing SonicWall automatycznie uaktualniany co minutę	Tak	Tak
Wsparcie 24/7	Tak	Tak
RMA (wymiana urządzenia)	Tak	Tak
Aktualizacje software/firmware	Tak	Tak
Subskrypcja antywirusa – opcja		
Sygnatury z wiodących w branży antywirusowych baz danych	Tak	Tak
Antywirus SonicWall TimeZero	Tak	Tak
Detekcja zombie	Tak	Tak
Subskrypcja Compliance – opcja		
Kompleksowe zarządzanie politykami	Tak	Tak
Skanowanie załączników	Tak	Tak
Dopasowywanie Record ID	Tak	Tak
Słowniki	Tak	Tak
Skrzynki do zatwierdzania/workflow	Tak	Tak
Archiwizowanie poczty	Tak	Tak
Raportowanie zgodności z przepisami	Tak	Tak
Subskrypcja szyfrowania - opcja		
Subskrypcja funkcji Compliance oraz oparte na politykach szyfrowanie i bezpieczna wymiana poczty	Tak	Tak

URZĄDZENIA EMAIL SECURITY	5000	7000	9000
Domeny		Bez ograniczeń	
System operacyjny		Hardened SonicWall Linux OS appliance	
Obudowa rackowa	1RU	1RU	1RU
CPU	Celeron G1820	i3-4330	E3-1275 v3
RAM	8 GB	16 GB	32 GB
Dyski	500 GB	1 TB	1 TB
Redundant disk array (RAID)	—	RAID 1	RAID 5
Dyski hot swap	Nie	Tak	Tak
Redundantne zasilanie	Nie	Nie	Tak
SAFE Mode Flash	Tak	Tak	Tak
Wymiary	17.0 x 16.4 x 1.7 in 43.18 x 41.59 x 4.44 cm	17.0 x 16.4 x 1.7in 43.18 x 41.59 x 4.44 cm	27.5 x 19.0 x 3.5 in 69.9 x 48.3 x 8.9 cm
Waga	16 lbs / 7.26 kg	16 lbs / 7.26 kg	50.0 lbs/ 22.7 kg
Waga WEEE	16 lbs / 7.37 kg	16 lbs / 22.2 kg	48.9 lbs/ 22.2 kg
Zużycie energii (W)	46	48	158
BTU	155	162	537
MTBF @25C w godzinach	130,919	150,278	90,592
MTBF @25C w latach	14.9	17.2	10.3
EMAIL SECURITY SOFTWARE			
Domeny		Bez ograniczeń	
System operacyjny		Microsoft Hyper-V Server 2012 (64-bit) lub nowszy Windows Server 2008 R2 lub nowszy, wyłącznie x64-bit	
CPU		Procesor Intel lub AMD 64-bit	
RAM		8 GB w konfiguracji minimalnej	
Wymagane miejsce na dysku		160 GB w konfiguracji minimalnej	
EMAIL SECURITY VIRTUAL APPLIANCE			
Wirtualizator		ESXi™ i ESX™ (wersja 5.0 i nowszy)	
Zainstalowany system operacyjny		8 GB (expandable)	
Alokowana pamięć operacyjna		4 GB	
Rozmiar dysku dla appliance		160 GB (expandable)	
Kompatybilność sprzętowa VMware		http://www.vmware.com/resources/compatibility/search.php	

USŁUGI PARTNERÓW SONICWALL

Potrzebujesz pomocy w zaplanowaniu, wdrożeniu lub optymalizacji rozwiązania SonicWall? Partnerzy SonicWall Advanced Services są przeszkoleni w zakresie świadczenia profesjonalnych usług na najwyższym poziomie. Dowiedz się więcej na stronie www.sonicwall.com/PES.

Email Security – informacje dotyczące zamówień

Urządzenia SonicWall Email Security

Produkt	SKU
Sonicwall Email Security Appliance 9000	01-SSC-7605
Sonicwall Email Security Appliance 7000	01-SSC-7604
Sonicwall Email Security Appliance 5000	01-SSC-7603
SonicWall Email Security Software	01-SSC-6636
SonicWall Email Security Virtual Appliance	01-SSC-7636

Subskrypcje SonicWall Email Security

Subskrypcje	SKU
Subskrypcja SonicWall Email Protection	
SonicWall Email Protection Subscription and 24X7 Support 25 Users - 1 Server (1yr)	01-SSC-6669
SonicWall Email Protection Subscription and 24X7 Support 1,000 Users - 1 Server (1yr)	01-SSC-6678
SonicWall Email Protection Subscription and 24X7 Support 10,000 Users - 1 Server (1yr)	01-SSC-6730
Subskrypcja SonicWall Email Anti-Virus	
SonicWall Email Anti-Virus 25 Users - 1 Server (1yr)	01-SSC-6759
SonicWall Email Anti-Virus 1,000 Users - 1 Server (1yr)	01-SSC-6768
SonicWall Email Anti-Virus 10,000 Users - 1 Server (1yr)	01-SSC-7562
Subskrypcja SonicWall Email Encryption	
SonicWall Email Encryption Service 25 Users (1yr)	01-SSC-7427
SonicWall Email Encryption Service 1,000 Users (1yr)	01-SSC-7471
SonicWall Email Encryption Service 10,000 Users (1yr)	01-SSC-7568
Subskrypcja SonicWall Email Compliance	
SonicWall Email Complaince Service 25 Users - 1 Server (1yr)	01-SSC-6639
SonicWall Email Complaince Service 1,000 Users - 1 Server (1yr)	01-SSC-6648
SonicWall Email Complaince Service 10,000 Users - 1 Server (1yr)	01-SSC-6735
Subskrypcja SonicWall TotalSecure Email	
SonicWall TotalSecure Email Subscription 25 Users (1yr)	01-SSC-7399
SonicWall TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-7398
SonicWall TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-7405
Subskrypcja Capture ATP Add-on for TotalSecure Email	
Capture ATP for SonicWall TotalSecure Email Subscription 25 Users (1yr)	01-SSC-1526
Capture ATP for SonicWall TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-1874
Capture ATP for SonicWall TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-1883
Subskrypcja SonicWall Advanced TotalSecure Email (w tym Capture ATP)	
SonicWall Advanced TotalSecure Email Subscription 25 Users (1yr)	01-SSC-1886
SonicWall Advanced TotalSecure Email Subscription 1,000 Users (1yr)	01-SSC-1904
SonicWall Advanced TotalSecure Email Subscription 10,000 Users (1yr)	01-SSC-1913

Pakiety i subskrypcje SonicWall Email Security Appliance są dostępne dla 25, 50, 100, 250, 500, 1000, 2000, 5000 i 10 000 użytkowników na 1 rok, 2 lub 3 lata. Dostępna jest także opcja wsparcia 8X5. Pełne listy SKU są dostępne u lokalnych resellerów SonicWall.

O firmie SonicWall

W erze hiper-rozproszonego środowiska pracy, gdy wszyscy są zdalni, mobilni i niechronieni, SonicWall konsekwentnie wprowadza w życie swoją koncepcję Boundless Cybersecurity. Zapewniając wgląd w czasie rzeczywistym i niezwykle ekonomiczne podejście do ochrony, SonicWall wypełnia luki w zabezpieczeniach w przedsiębiorstwach, instytucjach rządowych oraz małych i średnich firmach na całym świecie. Aby uzyskać więcej informacji, odwiedź stronę www.sonicwall.com oraz śledź nas w serwisach Twitter, LinkedIn, Facebook I Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Więcej informacji na stronie:
www.sonicwall.com

© 2020 SonicWall Inc. ALL RIGHTS RESERVED. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

DataSheet-EmailSecurityAppsAndSoftware-US-COG-2150

SONICWALL®